NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

ROBERT C. CHRISTIE,	:	
	:	Civ. Action No. 16-6572 (FLW)
Plaintiff,	:	
	:	
v.	:	**OPINION**
	:	
NATIONAL INSTITUTE FOR NEWMAN STUDIES, *et al.*,	:	
	:	
Defendants.	:	
	:	

WOLFSON, United States District Judge:

Plaintiff Robert C. Christie ("Plaintiff" or "Christie") was employed by defendant National Institute for Newman Studies ("NINS") as the company's Executive Director. When his employment ended, Plaintiff brought this suit, accusing NINS, and its two members of the board of directors, defendants Catherine Ryan and Drew Morgan (together with NINS, "Defendants"), of intentionally accessing, and deleting, his computer files and personal emails. Plaintiff alleges that Defendants' conduct violated the Computer Fraud and Abuse Act ("CFAC"), the New Jersey Computer Related Offenses Act ("NJCROA"), the Stored Communications Act ("SCA"), as well as invaded his privacy. In the instant matter, Defendants move for summary judgment on all counts, and Plaintiff cross-moves for partial summary judgment as to his invasion of privacy and SCA

claims.[1] Plaintiff also moves for summary judgment on Defendants' counterclaims. For the reasons set forth below, Defendants' motion is **GRANTED**, and Plaintiff's cross-motion for summary judgment as to his claims is **DENIED**. Plaintiff's motion for summary judgment as to Defendants' counterclaims is **GRANTED** in part and **DENIED** in part, as follows: Defendants' replevin and bailment counterclaims survives summary judgment; however, their unjust enrichment counterclaim is dismissed.

BACKGROUND

The facts recounted below are undisputed unless noted otherwise. In and around May 2015, Christie was hired as an Executive Director of the NINS, responsible for "the overall management of the operation" at the Institute. Defendants' Statement of Undisputed Facts ("Defs' Facts"), ¶ 4; Plaintiff's Statement of Undisputed Facts ("Pl.'s Facts"), ¶ 1. As the Executive Director, Christie supervised the entire NINS staff, as well as implemented employment and company policies. Defs' Facts, ¶¶ 5-7. In addition, in order to perform work related tasks, Christie was provided with a company desktop and laptop, both of which ran a version of Apple's

[1] Initially, Plaintiff only moved for partial summary judgment on his common law claim for invasion of privacy and the SCA claim. However, in Plaintiff's opposition to Defendants' motion, he indicates that he is seeking summary judgment on all remaining counts, *i.e.*, CFAA and NJCROA claims. While that request is procedurally defective, because in this Opinion, I grant Defendants' motion for summary judgment, I will nevertheless consider Plaintiff's cross-motion for summary judgment on all counts.

Macintosh OS X Operating system. *Id.* at ¶ 10. There is no dispute by Christie that these computers were owned by NINS, and at no time, did he have ownership of them. *Id.* at ¶¶ 11, 13. In fact, the same desktop computer had been used by a former executive director, Kevin Mongrain. *Id.* at ¶ 12.

NINS maintained e-mail accounts at the ninsdu.org domain, hosted by Google. *Id.* at ¶ 19. At the time Christie was employed by NINS, Mary Jo Dorsey was an administrator of NINS's email accounts, and she also provided general technical support to the NINS staff, including Christie. *Id.* at ¶¶ 16, 20. Christie was given an e-mail account at the ninsdu.org domain, rchristie@ninsdue.org, for work purposes. *Id.* at ¶ 21. In that connection, both of Christie's work computers, *i.e.*, desktop and laptop, were configured to download e-mails sent to Christie's work e-mail address. *See id.* at ¶ 22.

Christie also maintains a personal e-mail account at r.christie@att.net, which was hosted by Yahoo!. *Id.* at ¶¶ 23-24. These e-mails were stored on one or more of Yahoo!'s remote servers. *Id.* at ¶ 24. In June 2015, soon after Christie assumed his role as the Director, he e-mailed Dorsey "to unravel a problem" he was having with his personal e-mail, as he could not open those emails on either of the Apple computers. *See* E-Mail between Christie and Dorsey, dated June 3, 2015. A few minutes later, Dorsey responded: "Let's talk. I'll be able to better evaluate if I look at your computer and watch you walk through the process of

logging in." *Id.* On that same day, the desktop computer was synchronized with the r.christie@att.net e-mail account, such that Christie was able to access his personal e-mails on his work desktop computer. *Id.* at ¶ 28; Christie Tr., T98: 7-10; Pl.'s Facts, ¶ 2 ("[Christie's] att.net personal email account and his ninsdu.org email account were 'created' on the desktop Christie used at NINS.").

During the first half of 2016, Christie ceased providing services to NINS, *see* Defs' Facts, ¶ 34, and he was terminated from employment in April 2016. Pl.'s Facts, ¶ 3. Upon termination, Dorsey disabled the rchristie@ninsdu.org e-mail address. Defs' Facts, ¶ 35. Thereafter, Christie and NINS entered into negations regarding a severance agreement. Christie negotiated with Ryan, NINS' co-founder and officer. Pl.'s Facts, ¶ 5. According to Christie, he and Ryan came to an agreement on the terms in early June 2015, and Christie received a draft of the settlement agreement on June 16, 2016.

Around the time of the negotiations, in June 2016, NINS needed certain information regrading the dates of an upcoming scholarly conference, the Newmanfest, that NINS was holding with Father Ian Ker. Defs' Facts, ¶ 38. NINS attempted to reach Christie to obtain that information. *See* Pl.'s Facts ¶ 6. In fact, on June 8, 2016, Kenneth Parker, the newly named interim executive director, who replaced Christie, emailed Christie and requested that he "confirm the dates Fr. Ker has agreed to be at NINS and lecture." *Id.* In the same email, Parker requested

Christie to return the NINS keys and MacAir laptop to the Institute.[2] *Id.* Two days later, Christie responded that he was "working on the data that [he had] on the NINS [laptop,]" and that "it would take [him] some time to do so." *Id.* at ¶ 7. Parker, again, asked Christie to confirm "the dates that Fr. Ker arranged with [him.]" *Id.* at ¶ 11. On June 9, 2016, Christie responded that he would "ferret that information out and get it to [Parker] within the next few days, if not before then." *Id.* at ¶ 12.

Because NINS was unable to obtain certain information from Christie, on June 15, 2019, NINS held a staff meeting wherein the following people attended: McIntyre, Carol DeClaudio, Julia Morratto, Dorsey and Donna Lewis, and Father Morgan, who was a founding member and president of NINS. *Id.* at ¶ 15. Parker, located in England at the time of the meeting, also participated by video conferencing. At that meeting, McIntyre, as the office manager, sought and obtained permission from Parker and Father Morgan to access the NINS's desktop that was once used by Christie, in order to locate the dates on which Father Ker was

---

[2] In an email dated June 8, 2016, Parker stated to Ryan that Mia McIntyre, the office manager at NINS, had requested Christie to return "the computer and keys some time ago and received no response." Pl.'s Facts, ¶ 8 (citing Email from Ryan to Parker and McIntyre, dated June 8, 2016). Parker indicated that he preferred those items to be returned "with all due speed," as "[t]he documents on the computer are needed now. [Christie] is holding material that is needed for external review and for other urgent matters. Without access, [NINS] continue[s] to be in the dark about issues that are pressing." *Id.* As such, in addition to Parker, Ryan also emailed Christie, on June 9, 2016, asking Christie to return the NINS items, including the laptop, by June 13, 2016. *See id.* at ¶ 9 (citing Email from Ryan to Christie, dated June 9, 2016).

coming to NINS by reviewing Christie's work emails. *See id.* at ¶ 15; Defs' Facts, ¶ 40. According to McIntyre, Christie, in May 2016, provided McIntyre the password to the NINS desktop such that the incoming director could begin using that desktop. Defs' Facts, ¶¶ 36-37. However, Christie, on the other hand, claims that he provided his password to Father Morgan for a purpose unrelated to accessing the NINS desktop; according to Christie, the only password he gave was the one to the NINS' ADP account, and that password was the same one used for the desktop computer. Pl.'s Facts, ¶ 19.

To allow the search, Dorsey, first, re-enabled the rchristie@ninsdu.org e-mail account. Defs' Facts, ¶ 48. McIntyre unlocked the desktop with Christie's password, and proceeded to open Apple's e-mail application. *Id.* at ¶ 51. When the program opened, McIntyre was provided with a window including a listing for NINS, corresponding to the Christie's work e-mail account, as well as other listings. *Id.* at ¶ 52. McIntyre clicked on the work account to access e-mails from the rchristie@ninsdu.org address. *Id.* In order to search for particular e-mails, McIntyre typed in Ian Ker's name in the search box to attempt to retrieve relevant e-mails regarding the date that Father Ker could come to NINS. *Id.* at ¶ 53; Pl.'s Facts, ¶ 24. While McIntyre found the relevant information through the search, she also reviewed other e-mails in the process. Indeed, according to McIntyre, she identified an e-mail that contained negative comments about NINS from Christie to

another person; unbeknownst to McIntyre, this particular e-mail originated from Christie's personal account associated with the r.christie@att.net address. *Id.* at ¶ 56 (citing McIntyre Dep., T51:17-52:2). Thereafter, McIntyre stopped her search, which took approximately less than half an hour, and sent an e-mail to Parker requesting instructions.[3] *Id.* at ¶ 57.

Meanwhile, Parker was in Birmingham, England. *Id.* at ¶ 58. On the evening of June 15, 2016, Birmingham time,[4] Parker received an email from Christie with the scheduling information for Father Ker; however, according to Parker, because of the international time difference and other connectivity issues, Parker did not check his e-mail account until late in the afternoon, Birmingham time, on June 16, 2016. *Id.* at ¶¶ 59-61. Upon checking, Parker forwarded Christie's e-mail with the relevant dates to McIntyre at 6:50 p.m., or 1:50 p.m. Eastern Standard Time, and in the same message, instructed McIntyre to forward the e-mail containing negative comments about NINS made by Christie to Father Morgan. *Id.* at ¶ 62.

After Christie left his employment at NINS, he took the work laptop with him, and it was not returned until sometime during the course of this

---

[3] As discussed *infra*, by relying on his expert report, Christie argues that, on June 16, 2016, NINS, through McIntyre, "accessed" additional e-mails from Christie's personal att.net account, including some e-mails that were attorney-client privileged.

[4] Birmingham is five hours ahead of Eastern Standard Time.

litigation. In addition to accusations of unauthorized access of the NINS desktop computer and his personal e-mail account, Christie claims that a large swath of files were deleted from the laptop. In that regard, he accuses NINS of remotely accessing the laptop for the purposes of deleting files. Moreover, Christie claims that because of NINS's unauthorized access of his files and the resultant e-mails that were reviewed by NINS, the severance agreement was ultimately terminated by NINS in bad faith. *See* Pl.'s Facts, ¶ 31. Indeed, on June 17, 2016, NINS's attorney, David J. McAllister, corresponded with Christie, and in his email to Plaintiff, McAllister stated that "[NINS's] decision to withdraw the offer was made in large part due to the content of [Christie's] emails to Father Ian Ker." *Id.* at ¶ 32 (citing Email from McAllister to Christie, dated June 17, 2016).

Plaintiff brought suit against Defendants, asserting that they violated: (i) the CFAA; (ii) the NJCROA; and (iii) the SCA, as well as invaded Plaintiff's privacy. In response to Plaintiff's claims, Defendants asserted the following counterclaims: (i) replevin; (ii) bailment; and (iii) unjust enrichment. These counterclaims are based on the allegation that Plaintiff wrongfully retained the NINS's laptop computer and deprived NINS of the use of its laptop.

In the instant matters, Defendants move for summary judgment on all claims, and Plaintiff cross-moves for summary judgment. Plaintiff also moves for summary judgment on Defendants' counterclaims.

DISCUSSION

I. Standard of Review

Summary judgment is appropriate "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ .P. 56(c). A factual dispute is genuine only if there is "a sufficient evidentiary basis on which a reasonable jury could find for the non-moving party," and it is material only if it has the ability to "affect the outcome of the suit under governing law." *Kaucher v. County of Bucks*, 455 F.3d 418, 423 (3d Cir. 2006); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). Disputes over irrelevant or unnecessary facts will not preclude a grant of summary judgment. *Anderson*, 477 U.S. at 248. "In considering a motion for summary judgment, a district court may not make credibility determinations or engage in any weighing of the evidence; instead, the non-moving party's evidence 'is to be believed and all justifiable inferences are to be drawn in his favor.'" *Marino v. Indus. Crating Co.*, 358 F.3d 241, 247 (3d Cir. 2004) (quoting *Anderson*, 477 U.S. at 255)); *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587, (1986); *Curley v. Klem*, 298 F.3d 271, 276-77 (3d Cir. 2002).

The party moving for summary judgment has the initial burden of showing the basis for its motion. *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). "If the moving party will bear the burden of persuasion at trial,

that party must support its motion with credible evidence . . . that would entitle it to a directed verdict if not controverted at trial." *Id.* at 331. On the other hand, if the burden of persuasion at trial would be on the nonmoving party, the party moving for summary judgment may satisfy Rule 56's burden of production by either (1) "submit[ting] affirmative evidence that negates an essential element of the nonmoving party's claim" or (2) demonstrating "that the nonmoving party's evidence is insufficient to establish an essential element of the nonmoving party's claim." *Id.* Once the movant adequately supports its motion pursuant to Rule 56(c), the burden shifts to the nonmoving party to "go beyond the pleadings and by her own affidavits, or by the depositions, answers to interrogatories, and admissions on file, designate specific facts showing that there is a genuine issue for trial." *Id.* at 324; *see also Matsushita*, 475 U.S. at 586; *Ridgewood Bd. of Ed. v. Stokley*, 172 F.3d 238, 252 (3d Cir. 1999). In deciding the merits of a party's motion for summary judgment, the court's role is not to evaluate the evidence and decide the truth of the matter, but to determine whether there is a genuine issue for trial. *Anderson*, 477 U.S. at 249. Credibility determinations are the province of the factfinder. *Big Apple BMW, Inc. v. BMW of N. Am., Inc.*, 974 F.2d 1358, 1363 (3d Cir. 1992).

There can be "no genuine issue as to any material fact," however, if a party fails "to make a showing sufficient to establish the existence of an element essential to that party's case, and on which that party will bear the burden of proof at trial." *Celotex*, 477 U.S. at 322-23. "[A] complete

failure of proof concerning an essential element of the nonmoving party's case necessarily renders all other facts immaterial." *Id.* at 323; *Katz v. Aetna Cas. & Sur. Co.*, 972 F.2d 53, 55 (3d Cir. 1992).

II. The Computer Fraud and Abuse Act

At the outset, before I set forth the relevant standard under the CFAA, I note that the statute has various provisions prohibiting the intentional, unauthorized access of protected computers. *See* 18 U.S.C. § 1030(a)(1)-(7). These provisions prohibit certain enumerated conduct. *See P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir. 2005); *Advanced Fluid Sys. v. Huber*, 28 F. Supp. 3d 306, 326 (M.D. Pa. 2014) ("The CFAA prohibits seven types of computer crimes involving unauthorized access to computers (or access in excess of authorization) which results in obtaining information from or damaging the computer."). Indeed, "to state a civil claim for violations of the CFAA, a plaintiff must allege: (1) damage or loss 'to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value';[5] (2)

[5] Pursuant to § 1030(g), "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [subclause] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." 18 U.S.C. § 1030(g). Relevant to this matter, § 1030(c)(1)(A)(I) provides that to sustain a civil suit under § 1030(a), the alleged wrongful conduct must have caused a loss of at least $5,000 in value. While Defendants argue that they are entitled to summary judgment on the CFAA claim because, *inter alia*, Plaintiff failed to established any damages, I do not need to reach the issue of loss, however, because I find that Plaintiff has not submitted

caused by; (3) violation of one of the substantive provisions of §§ 1030(a) or (b)." *Advanced Fluid*, 28 F. Supp. 3d at 326 (quoting *Sealord Holdings, Inc. v. Radler*, No. 11-6125, 2012 U.S. Dist. LEXIS 29878, at *11-12 (E.D. Pa. Mar. 6, 2012)).

Notwithstanding these various provisions under the CFAA, Plaintiff, in his Amended Complaint, does not specify under which provision he is proceeding. While Defendants, in their briefing, cited §1030(a)(5)(B), Plaintiff, on the other hand, points to § 1030(a)(2)(C). Regardless of which provision, however, the essential element of all § 1030(a) claims is the "unauthorized" access of information in connection with computers. *See Collegesource, Inc. v. Academyone, Inc.*, 597 Fed. Appx. 116, 129 (3d. Cir. 2015)("Common to all . . . claims under the CFAA is the requirement of proof that the defendant accessed information 'without authorization' or 'exceed[ed] authorized access.'").[6] Because I find that Plaintiff has failed

---

sufficient evidence to show that Defendants accessed information without authorization.

[6] In order to recover under the CFAA, Plaintiff must prove that the computers that he alleges were accessed without authorization by Defendants were "protected computers" under the meaning of the statute. That term is defined as a computer –

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located

to show a genuine issue of material fact as to that particular element, my analysis focuses on that inquiry.

The CFAA is a criminal statute which penalizes a range of computer offenses and also provides a civil remedy in certain circumstances to persons who suffer damage or loss as a result of a violation of its provisions. *See* 18 U.S.C. § 1030(g) (specifying the circumstances in which a plaintiff may bring a civil action under the CFAA); *Grant Mfg. & Alloying, Inc. v. McIlvain*, No. 10-1029, 2011 U.S. Dist. LEXIS 108961, at *10 (E.D. Pa. Sep. 23, 2011). In general, the CFAA prohibits the knowing or purposeful unauthorized access to, or transmission of, protected computer data. *See* 18 U.S.C. § 1030(a); *Grant Mfg. & Alloying, Inc. v. McIlvain*, 499 Fed. Appx. 157, 159 (3d Cir. 2012). The touchstone of a CFAA claim is the "unauthorized" access of computers. *See*, *e.g.*, 18 U.S.C. § 1030(a)(2)(C) ("intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer"); § 1030(a)(4) ("knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains

---

> outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]

18 U.S.C. 1030(e)(2)(A), (B). The parties do not dispute, on their motions, that NINS's computer and the laptop are "protected computers" encompassed by the CFAA.

anything of value . . ."); § 1030(a)(5)(C) ("intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss . . .").

In the employment context, "[a]n employee accesses a computer 'without authorization' when he [or she] 'has no rights, limited or otherwise, to access the computer in question.'" *Synthes, Inc. v. Emerge Med., Inc.*, No. 11-cv-1566, 2012 U.S. Dist. LEXIS 134886, at *52 (E.D. Pa. Sep. 19, 2012) (quoting *Grant Mfg.*, 2011 U.S. Dist. LEXIS 108961, at *24); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)("an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it"); *United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991) (holding that the word "authorization" for purposes of the CFAA is "of common usage, without any technical or ambiguous meaning"); *Collegesource,* 597 Fed. Appx. at 129. Simply put, a person accesses a computer without authorization when he or she does so "without sanction or permission." *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011).

Importantly, an employee who accesses a computer by the terms of his or her employment is "authorized" to use that computer for purposes of the CFAA even if the purpose in doing so is to misuse or misappropriate the information. *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 407 (E.D. Pa. 2009); *see, e.g.*, *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322 (N.D. Ga. 2007); *Brett Senior & Assocs., P.C. v. Fitzgerald*,

No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at *2-4 (E.D. Pa. Jul. 13, 2007); *Lockheed Martin Corp. v. Speed*, No. 05-31, 2006 U.S. Dist. LEXIS 53108, at *5 (M.D. Fla. Aug. 1, 2006); *Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 495 (D. Md. 2005); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008). In other words, what one intends to do with information taken from a computer is irrelevant if the individual was given computer access to that information. *See QVC, Inc. v. Resultly, LLC*, 159 F. Supp. 3d 576, 595 (E.D. Pa. 2016)("[T]hose who have permission to access a computer for any purpose, such as employees, cannot act 'without authorization' unless and until their authorization to access the computer is specifically rescinded or revoked.").

Moreover, whether an employee "exceed[s] authorized access depends on the computer access restrictions imposed by his employer." *Grant Mfg.*, 2011 U.S. Dist. LEXIS 108961, at *24. For purposes of the CFAA, a person "exceeds authorized access" by "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accesser is not entitled to obtain or alter." 18 U.S.C. § 1030(e)(6). As this definition makes clear, an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has "exceed[ed] authorized access." *LVRC Holdings*, 581 F.3d at 1133; *see Collegesource*, 597 Fed. Appx. at 129.

Here, on these summary judgment motions, the parties point the Court to three different types of access: (1) the NINS's desktop computer; (2) the NINS's laptop computer; and (3) Plaintiff's Yahoo! e-mails. Plaintiff argues that Defendants violated the CFAA when they accessed these "computers" without his authorization. Before I address the parties' substantive arguments, I turn first to Plaintiff's pleadings. Notably, Plaintiff alleges that the sole basis of his CFAA claim is the unauthorized access of his Yahoo! e-mails. *See* Am. Compl., ¶¶ 27-34 ("NINS knowingly and intentionally accessed Plaintiff's personal email account with AT&T which is hosted by Yahoo! servers without Plaintiff's authorization"). Plaintiff has not sought to amend his Amended Complaint to include the NINS's desktop or laptop, and he cannot do so in his cross-motion for summary judgement. *See Bell v. City of Phil.*, 275 Fed. Appx. 157, 160 (3d Cir. 2008). As such, as it stands now, Plaintiff's CFAA claim is only based on his complaint that Defendants wrongfully accessed his Yahoo! e-mails.

The problem with Plaintiff's claim is that the CFAA does not protect the unauthorized access of emails. Rather, as I have discussed above, the statute only protects the "unauthorized" access of *computers*, not stored electronic communication in the form of e-mails. In other words, critically, "the CFAA is aimed at unauthorized access to computers, not unauthorized access to web-based accounts." *Owen v. Cigna*, 188 F.

Supp. 3d 790, 793 (N.D. Ill. 2016)(citing 18 U.S.C. § 1030(a)(2));[7] *See Brooks Group & Assocs. v. LeVigne*, No. 12-2922, 2014 U.S. Dist. LEXIS 52479, at *28-29 (E.D. Pa. Apr. 15, 2014) ("The CFAA protects people from unauthorized access to computers, for example by hacking or stealing a password."); *see also Sloan Fin. Group, LLC v. Coe*, No. 09-2659, 2010 U.S. Dist. LEXIS 122600, at *16 (D.S.C. Nov. 18, 2010)("[W]hether or not it was a violation of company policy, emailing the spreadsheets did not involve accessing a computer 'without authorization' under the CFAA."). Accordingly, Plaintiff's claim, as pled, is simply beyond the scope of the CFAA, and summary judgment can be granted on that claim based on this reason, alone.

Even if I were to treat Plaintiff's Amended Complaint as having included allegations regarding the NINS's desktop and laptop computers, his CFAA claim would still fail as a matter of law, for the simple reason that Plaintiff did not have ownership of those devices. A majority of the cases involving the CFAA, in the context of employment, involve claims asserted by *employers* against employees for the unauthorized access of company computers; this case is the reverse — Plaintiff, a former employee, alleging that NINS and its officers and directors, Christie's former employer, accessed their own company computers without

[7] Indeed, the title of section 1030 – "Fraud and Related Activity in Connection with Computers" — expressly identifies this distinction.

Plaintiff's authorization. In this Court's research, I found only one case which resembles the instant matter.

In *Owen*, the plaintiff, a former employee of defendant company, Professional Consultants, Inc., claimed that the company, and its officers and directors, violated multiple federal laws, including the CFAA, when they accessed her private e-mail account through her former work computer. *Owen*, 188 F.Supp. 3d at 791. Defendants moved to dismiss on the grounds that they had authorization to access their own computers. The court agreed, explaining:

> Neither party has identified—and the Court has not found—any CFAA case involving an employee's claim that her former employer exceeded its authority to access its own computer . . . . None of Owen's allegations suggests that she retained any authority to grant or deny anyone permission to access her former work computer after she left PCI. She may well have had the power to deny access to her web-based email account, but the CFAA is aimed at unauthorized access to computers, not unauthorized access to web-based accounts, see 18 U.S.C. § 1030(a)(2), and the only computer Owen alleges Defendants accessed without authority is her former work computer. These allegations do not raise her claim above the speculative level, and Count II is dismissed for failure to state a claim upon which relief can be granted. This dismissal is with prejudice.

Id. at 793.

Just like *Owen*, Plaintiff, here, also brings a CFAA claim, alleging that his former employer accessed the work desktop and laptop without authorization. But, Plaintiff has conceded that he does not own those computers; indeed, the desktop computer was, at all times, located in NINS's headquarter, and while Plaintiff kept the laptop for a period of time,

it has been returned to NINS during the pendency of this litigation. Simply put, the record is clear that Plaintiff has no ownership of either device. Without having ownership, Plaintiff cannot, as a legal matter, exert control, such that he can exclude others from accessing the devices. Instead, because NINS is the rightful owner of those machines, consistent with its ownership rights, NINS has the authority to decide who has access. *See, e.g., Skapinetz v. CoesterVMS.com, Inc.*, No. 17-1098, 2018 U.S. Dist. LEXIS 21648, at *16-17 (D. Md. Feb. 9, 2018). This is so even if Plaintiff locked the desktop with a personal password. Accordingly, because Plaintiff cannot exercise any ownership rights over the devices, he cannot, as a threshold matter, accuse Defendants of violating the CFAA by accessing computers that they own. To adopt Plaintiff's position would not only gravely expand the scope of the CFAA, but also common law concepts of property rights. Thus, as a matter of law, summary judgment can be granted on this basis as to Plaintiff's CFAA claim relating to the unauthorized access of the NINS desktop or the laptop.

Even assuming, *arguendo,* that Plaintiff can bring a CFAA claim, summary judgment would still be appropriate, because he cannot show that there is a genuine issue of material fact that Defendants lacked the proper authorization. I first address the alleged unauthorized access of the desktop and Yahoo! e-mails. Plaintiff maintains that NINS lacked authorization to access the NINS desktop computer, since it was password protected. In that regard, Plaintiff claims that McIntyre misused the

password that was given by Plaintiff to Father Morgan for the sole purpose of accessing the NINS' ADP account, which purpose, Plaintiff claims, is unrelated to computer access. As discussed *supra*, however, NINS did not require Plaintiff's authorization to access its own desktop computer, regardless whether it was protected by Plaintiff's personal password. Rather, Plaintiff was merely a user of the computer, which use was authorized in the first instance by NINS.[8] As such, when Parker and Father Morgan, on behalf of NINS, gave McIntyre permission, McIntyre was authorized to access the desktop computer, within the meaning of the CFAA.

Next, Plaintiff argues that he never authorized NINS to access his personal e-mail account either through the Yahoo! server or through the desktop computer. In that connection, Plaintiff argues that Defendants violated the CFAA when McIntyre read his personal Yahoo! mail while performing a search, and review, of his NINS e-mail account. I disagree. On its motion, Defendants proffered a report from David J Peck (the "Peck Report"), a computer forensic expert. Peck examined a forensic copy of the desktop and opined that when Christie asked a NINS employee, Dorsey, in

---

[8] Christie relies on the case *White v. White*, 344 N.J. Super. 211(Ch. Div. 2001), for the legal principle that "'without authorization' means using a computer from which one has been prohibited, or using another's password or code without permission." *Id.* at 221. The court in *White* dealt with the issue whether an authorized user of a jointly-used family computer had violated certain laws when a co-owner and co-user accessed the e-mails stored on that computer. That case is distinguishable because Christie, as he has conceded, does not own the computers at issue in this case.

2015 to assist him with accessing his personal e-mail on the desktop computer, that very day, "the desktop began downloading [e-mail] messages from the remote server hosting r.christie@att.net, in a manner consistent with Christie's request." Peck Report, pp. 14-15. The expert further stated the following:

> [W]hen the NINS desktop was booted up and the Mail application opened in June of 2016, the Mail application on the NINS desktop would have contained all the fetched e-mails from r.christie@att.net. NINS was not required to take any purposeful action to download these e-mails, and was not required to establish a connection to the remote server storing the e-mails. Any access to the remote server, and any retrieval of e-mail messages from that server, was managed by the synchronization that had been set up on June 3, 2015, the same day Christie requested it, and never disabled. Instead, NINS could view e-mails sent or received using the r.christie@att.net e-mail account without accessing the remote server by accessing copies already stored locally on the NINS Desktop.

Id. at p. 17.

Put differently, according to Peck, when McIntyre was given access to search through Christie's work e-mails on the NINS desktop, Christie's personal Yahoo! e-mail account automatically connected to the desktop computer and downloaded Christie's personal e-mails stored on Yahoo!'s remote server. Importantly, Plaintiff's own expert on this subject, Tino Kyprianou, did not dispute this finding from Peck. Specifically, when explicitly asked at his deposition whether he found any inaccuracies in the Peck Report, Kyprianou stated: "No, I did not." Kyprianou Dep., T9:14-22.

Notwithstanding the forensics evidence, Plaintiff insists that he never authorized NINS to maintain his personal e-mails on the work

desktop, and he has certified, on this motion, that no such authorization was provided. However, Plaintiff admits that the NINS desktop was "configured to synchronize with the r.christie@att.net e-mail account." Plf.'s Statements in Response to Defs' Statement of Undisputed Facts, ¶ 28. And, Plaintiff has also admitted that he used the desktop computer to access his r.christie@att.net account. Pl.s' Dep. T98:7-10. What Plaintiff disputes is that other than asking Dorsey for assistance to view his personal e-mails, he never requested his e-mails be automatically downloaded from the Yahoo!'s remote servers. While Plaintiff claims that he never requested this process to take place, the undisputed fact remains, however, that when the synchronization was initiated in June 2015, that set-up began the automatic downloading process, which was never disabled by Plaintiff or any of the NINS staff. That fact was confirmed by both experts. As such, because the synchronization was automatic, none of the NINS staff accessed the Yahoo! remote servers to download Plaintiff's e-mails.[9] Indeed, there is no evidence that McIntyre, or any of the

[9] In his briefing, Plaintiff argues that had he authorized the synchronization process to take place, he would have known that his personal e-mail was on the desktop and could have deleted the account upon his return to NINS in early June 2016. Plaintiff's argument in this regard is irrelevant; Plaintiff does not dispute that he — in fact — authorized the "synchronization" process. *See* Plf.'s Statements in Response to Defs' Statement of Undisputed Facts, ¶ 28. Indeed, it is undisputed that in order for that process to be successful, it required Plaintiff to enter his Yahoo! e-mail account password. And, Plaintiff has not disputed that he initially provided such a password to permit synchronizing of his Yahoo! e-mails to the NINS desktop. To the extent Plaintiff was not aware that the automatic synchronization would remain on the desktop, that lack of knowledge is not relevant to the issue of

individual defendants, accessed Plaintiff's personal e-mails directly through Yahoo!'s remote servers. Moreover, there is also no dispute that McIntyre was not aware that Plaintiff's personal e-mails were automatically synchronized with the NINS desktop, such that they could be viewed on that computer. Rather, the record is clear: McIntyre reviewed Plaintiff's work and synchronized personal e-mails on the NINS desktop, and there is no evidence that McIntyre intentionally, and without authorization, accessed Plaintiff's Yahoo! e-mails directly through a remote server.[10] Accordingly, once McIntyre was granted access by NINS to search through the desktop, Plaintiff's claim that the CFAA was violated because McIntyre viewed his personal e-mails without authorization is plainly not actionable under the statute; the CFAA only prohibits the "unauthorized" access of a computer by an employee, and here, the undisputed facts show that no such conduct occurred. Summary judgment on this aspect of the CFAA claim is granted.

Finally, Plaintiff accuses Defendants of violating the CFAA by remotely hacking into the NINS laptop and deleting hundreds of work and

---

whether McIntyre intentionally accessed Plaintiff's personal e-mails without authorization.

[10] As a last-ditch effort, Plaintiff argues that NINS's removal of the synchronization between his personal e-mail account and the desktop after having accessed his e-mails in June 2016, somehow is evidence that Defendants were aware that they did not have access in the first place. To the contrary, the fact that NINS removed the synchronization process after they became aware it, suggests that Defendants took the necessary steps to discontinue the process in order to prevent Christie's Yahoo! e-mails from being automatically download onto the NINS desktop.

personal e-mails and files. In response, Defendants deny accessing the laptop remotely or otherwise. First and foremost, I stress, again, that NINS does not require Plaintiff's authorization to access its own laptop. To the extent that NINS in fact accessed the laptop remotely, that conduct is not actionable under the CFAA. In any event, there is no evidence that any of the NINS staff committed such an act.[11]

I start with the testimony of the NINS staff: Dorsey, McIntyre, Parker, Ryan and Morgan all denied that they accessed the laptop computer remotely. *See* Dorsey Tr., T6:22-T7:2l; McIntyre Tr., T62:21-23; Parker Tr., T45:9-13; Ryan Tr., T63:5-10; Morgan Tr., T12:9-19, T23:21-24. Instead, Plaintiff relies on his expert and posits that "somebody accessed" the computer. Without any evidentiary support, Plaintiff asserts that because he, himself, did not delete the emails and files on the laptop, it must have been NINS. This is not appropriate evidentiary support on a summary judgment motion.

After analyzing the contents of the laptop, Plaintiff's expert determined that numerous emails, attachments, and address book entries were deleted from the laptop. *See* Kyprianou Report, p. 7. Kyprianou

---

[11] I note that as a matter of law, even if NINS deleted Plaintiff's emails and files on the laptop, it is still not a violation under the CFAA. As I have recounted extensively the scope of the CFAA, the statute only punishes those who access a computer without authorization. In that regard, when someone is authorized to access a computer, it is not within the purview of the CFAA's prohibited conduct when that authorized personnel misuses or misappropriates the information contained on that computer. *See*, *supra*.

opined that the deletion was unlikely caused by user error on Plaintiff's part.[12] Moreover, the expert "confirmed that the Remote Desktop Connection Application existed on the . . . LAPTOP," and that the application "allow[s] for the ability to remotely access the computers." *Id.* at p. 13. However, Kyprianou specifically states in his report that he "was unable to determine whether the LAPTOP was remotely accessed . . . and if so, who did so." *Id.* Rather, Kyprianou speculates that "it is plausible that a user with administrative rights accessed the LAPTOP to delete files and emails . . . ." *Id.* Kyprianou's testimony further sheds light on his opinion; when specifically questioned regarding NINS's role in the alleged "hacking," Kyprianou answered that he did not "find any evidence that NINS hacked into [the laptop]." Kyprianou Tr., T39:23-24. Moreover, he clarified that even though he found a desktop connection application on the laptop, it does not mean that it was utilized to remotely connect with the laptop from an outside source. *Id.* at T19:7-19. In fact, Kyprianou acknowledged that the application was bundled with Microsoft Office for Mac computers. *Id.* at T36:8-18. In other words, the expert agreed that the application in question — which would allow an outside user to remotely access the laptop — was pre-installed with Microsoft Office, not

[12] However, Kyprianou testified that he relied on Plaintiff's own assertion that Plaintiff did not delete, intentionally or otherwise, any files from the laptop, and that the expert was unable to confirm through direct forensic evidence that Plaintiff did not, in fact, delete any files. *See id.* at T11:19-T12:3.

necessarily intentionally installed by NINS to allow for remote access. *Id.* Damningly, having examined the forensic evidence, Kyprianou testified that he was unable to determine that the laptop was remotely accessed at all, albeit suggesting that perhaps someone accessed the laptop through untraceable means. *Id.* at T38:5-18.

The issue with Kyprianou's opinion is that he could not identify any credible evidence to establish with any degree of certainty that someone from NINS remotely accessed the laptop computer. Indeed, while the expert opines that someone "could" have accessed the laptop remotely, he cannot determine whether such access was actually performed. More importantly, even if remote access occurred, Kyprianou could not determine whether NINS did so. To defeat summary judgment, Plaintiff cannot reasonable rely on an expert who ultimately resorts to speculation. It is well established that, in the context of summary judgment motions, the Third Circuit has demanded that the factual predicate of an expert's opinion must find some support in the record, and has emphasized that mere "theoretical speculations" lacking a basis in the record will not create a genuine issue of fact. *Pa. Dental Ass'n. v. Med. Serv. Ass'n.*, 745 F.2d 248, 262 (3d Cir. 1984)(quotations omitted); *see Sharpe v. Robbins*, No. 07-1879, 2009 U.S. Dist. LEXIS 52792, at *10 (D.N.J. Jun. 23, 2009)("[a]n expert's opinion, however, must be supported by the factual evidence and not based solely on the expert's conclusions"); *Marvel v. Del. Cnty.*, No. 07-5054, 2009 U.S. Dist. LEXIS 46755, at *17 (E.D. Pa. June 2, 2009), *aff'd*

397 Fed. Appx. 785 (3d Cir. 2010)(finding that an expert report that merely offers conclusory opinions, without explicit factual foundation, is insufficient to defeat a motion for summary judgment); *Major League Baseball Props., Inc. v. Salvino, Inc.*, 542 F.3d 290, 311 (2d Cir. 2008)("[a]n expert's opinions that are without factual basis and are based on speculation or conjecture are similarly inappropriate material for consideration on a motion for summary judgment"); *Zeller v. J.C. Penney Co.*, No. 05-2546, 2008 U.S. Dist. LEXIS 25993, at *22 n.13 (D.N.J. Mar. 31, 2008)(noting that "an expert's bare conclusions are not admissible under" the Federal Rules of Evidence, and that the exclusion of an expert's opinion on a summary judgment motion is appropriate when that expert's "conclusions were to speculative"); *Edison Wetlands Ass'n, Inc. v. Akzo Nobel Chems., Inc.*, No. 08-419, 2009 U.S. Dist. LEXIS 119281, at *6-7 (D.N.J. Dec. 22, 2009)(holding that "the expert must have good grounds for his or her belief" and that courts "need not admit bare conclusions or mere assumptions proffered under the guise of expert opinions")(quotations and citations omitted); *Scott v. Calpin*, No. 08-4810, 2012 U.S. Dist. LEXIS 102644, at *24-25 (D.N.J. Jul. 24, 2012). On a summary judgment motion, Plaintiff must proffer more concrete evidence to show unauthorized access on the part of NINS, and because he has failed to do so after a lengthy discovery process, summary judgment on all aspect of Plaintiff's CFAA claim is appropriate.

III. New Jersey Computer Related Offenses Act

Consistent with his CFAA claim, Plaintiff also brought a companion state law claim under the NJCROA. The statute, in full, reads:

> A person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor in the Superior Court and may recover compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation:
>
> a. The purposeful or knowing, and ***unauthorized*** altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;
>
> b. The purposeful or knowing, and ***unauthorized*** altering, damaging, taking or destroying of a computer, computer system or computer network;
>
> c. The purposeful or knowing, and ***unauthorized*** accessing or attempt to access any computer, computer system or computer network;
>
> d. The purposeful or knowing, and ***unauthorized*** altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or
>
> e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

N.J.S.A. 2A:38A-3 (emphasis added). The statute imposes liability against an "actor" whose "purposeful or knowing" conduct is proscribed by the statute. Although the term "actor" is not defined within the act, "each subsection of [the Act] is independent of the other and each subsection

requires that the conduct by the actor be 'purposeful and knowing.'" *Fairway Dodge, L.L.C. v. Decker Dodge, Inc.*, 191 N.J. 460, 469 (2007).

Like his CFAA claim, Plaintiff does not identify under which subsection of the NJCROA he is proceeding.[13] Significantly, pursuant to the plain language of the statute, subsections (a) – (d) require an actor to access a computer, computer system, or network without authorization. *See Ferring Pharms. Inc. v. Watson Pharms., Inc.*, No. 12-5824, 2014 U.S. Dist. LEXIS 199073, at *17 (D.N.J. Aug. 4, 2014). Notably, the Third Circuit has advised that courts have interpreted the NJCROA "in harmony with its federal counterpart," the CFAA. *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 277 (3d Cir. 2016); *New London Assocs., LLC v. Kinetic Soc. LLC*, No. 18-7963, 2019 U.S. Dist. LEXIS 62731, at *23 (D.N.J. Apr. 11, 2019); *Mu Sigma, Inc. v. Affine, Inc.*, No. 12-1323, 2013 U.S. Dist. LEXIS 99538 (D.N.J. July 17, 2013) (dismissing claims under the state and federal computer statutes for identical reasons).

Here, having determined that under the CFAA, Plaintiff has failed to prove that Defendants did not have the adequate authorization to access their own laptop and desktop computers, for substantially similar reasons, I find that Plaintiff cannot prove his NJCROA claim as to the laptop and

[13] Similar to his CFAA claim, in the Amended Complaint, Plaintiff only alleges the accessing of his Yahoo! e-mails as the sole basis of his NJCROA cause of action. *See* Am. Compl., ¶ 40 ("Defendants violated N.J.S.A. 2A:38A-3 by purposely and knowingly accessing Plaintiff's email account without authorization while Plaintiff resided in New Jersey.").

the desktop. *See*, *supra*. Likewise, because Plaintiff has failed to prove that NINS and its staff accessed its Yahoo! e-mails directly through the Yahoo! remote servers, he cannot demonstrate that his personal e-mails were accessed without authorization. Accordingly, summary judgment is appropriate as to all aspects of Plaintiff's NJCORA claim, for the same reasons why Plaintiff's CFAA claim fails to survive on this motion.[14]

IV. Invasion of Privacy

Plaintiff's New Jersey common law claim of invasion of privacy is based on his allegations that Defendants wrongfully, and without authorization, accessed his Yahoo! e-mail account and read his personal e-mails. Plaintiff also alleges that Defendants invaded his privacy when they intentionally deleted Plaintiff's e-mails and files when they "hacked" into the NINS laptop. *See* Am. Compl., ¶ 37.

As a preliminary matter, based on the record, Plaintiff has failed to adduce sufficient evidence to prove that Defendants accessed his laptop when it was in his possession in New Jersey. *See*, *supra*. Because Plaintiff cannot establish unlawful access, his invasion of privacy claim, on the

---

[14] To the extent Plaintiff intends to proceed under subsection (e), based on his allegation that NINS deleted his e-mails and files on the NINS laptop, I also find that summary judgment is appropriate. As I have explained, in the context of the CFAA, Plaintiff has failed to demonstrate that NINS accessed the laptop remotely; the same reasoning applies with equal force as to this aspect of Plaintiff's NJCROA claim, and as such, without any evidence of access, Plaintiff cannot show that NINS "purposeful[ly] or knowing[ly] access[ed] and reckless[ly] alter[ed], damage[ed], destroy[ed] or obtain[ed] of any data . . . ." N.J.S.A. 2A:38-3(e).

basis of the deletion of e-mails and files on the NINS laptop, does not survive summary judgment. Furthermore, on his motion for partial summary judgment, Plaintiff clarifies that his privacy claim centers on NINS' conduct when McIntyre allegedly accessed and reviewed Plaintiff's personal e-mails. *See* Pl. Brief in Support of Partial Summary Judgement, p. 5. Plaintiff argues, however, that he had an expectation of privacy in the e-mails contained in his password protected personal Yahoo! e-mail account that was accessed and viewed by NINS. However, as I have discussed, *supra*, there is no evidence that any of the NINS' staff, including McIntyre, directly accessed Plaintiff's Yahoo! e-mail account using Plaintiff's password. Rather, McIntyre, during a search of the NINS desktop, reviewed certain of Plaintiff's personal e-mail correspondence that were automatically synchronized to the desktop. As such, the issue here is whether Plaintiff has shown that such limited conduct constitutes invasion of privacy. I answer that question in the negative.

In New Jersey, "the common law recognizes various causes of action relating to the right to privacy." *Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 95 (1992). New Jersey has adopted the Restatement (Second) of Torts, § 652B, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for the invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

White, 344 N.J. Super. at 222 (quoting The Restatement (Second) of Torts, § 652B); *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 316 (2010); *Bisbee v. John C. Conover Agency, Inc.*, 186 N.J. Super. 335, 339 (App. Div. 1982); *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 674 (D.N.J. 2013); Relevant here, the intentional invasion, or also known as intrusion of seclusion, may be by some "form of investigation or examination into [a person's] private concerns, as by opening [his/her] private and personal mail . . . . The intrusion itself makes the defendant subject to liability . . . ." *White*, 344 N.J. Super at 222 (quoting The Restatement (Second) of Torts, § 652B, comment b.). And, the intrusion must be "highly offensive to a reasonable person." *Id.* Whether it is "highly offensive" turns on one's reasonable expectation of privacy. In that regard, a "'reasonable person' cannot conclude that an intrusion is 'highly offensive' when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy." *Id.*

According to the New Jersey Supreme Court, "expectations of privacy are established by general social norms." *State v. Hempele*, 120 N.J. 182, 200 (1990). That means, one's expectation of privacy must be objectively reasonable. *State v. Brown*, 282 N.J. Super. 538, 547 (App. Div.) *cert. denied*, 143 N.J. 322 (1995). A person's subjective belief of privacy is "irrelevant." *Id.* "[W]hether an employee has a reasonable expectation of privacy in [his/her] particular work setting must be addressed on a case-by-case basis." *Stengart*, 201 N.J. at 317. In making

that determination, "a court must [decide] whether objectively, given the facts and circumstances of the particular case, a person would reasonably believe he has an expectation of privacy." *Poltrock v. NJ Auto. Accounts Mgmt. Co.*, No. 08-1999, 2008 U.S. Dist. LEXIS, at *16 (D.N.J. Dec. 22, 2008).

In sum, a claim for invasion of privacy succeeds if a plaintiff proves that (1) there was an intentional intrusion "upon the solitude or seclusion of another or his private affairs," and that (2) this intrusion would highly offend the reasonable person. *Bisbee*, 186 N.J. Super. at 339. Under the first prong, a defendant must commit an intrusive act. *See O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989) (according to the Restatement, an actor must "commit [an] intrusive act" to be liable for invasion of privacy). "The converse of this principle is, however, of course, that there is no wrong where defendant did not actually delve into plaintiff's concerns." *Bisbee*, 186 N.J. Super at 340. Importantly, a plaintiff faces a high burden in asserting a cause of action based on the tort of intrusion of seclusion. *Stengart*, 201 N.J. at 316-17.

Here, the alleged act of intrusion is a limited one: whether McIntyre's viewing of Plaintiff's personal e-mails that were downloaded to the NINS desktop is an intentional intrusion that would highly offend a reasonable person. That question turns on whether Plaintiff had a reasonable expectation of privacy in those e-mails, which requires a case-by-case analysis. The undisputed facts reveal that McIntyre was granted the

authorization to access the NINS desktop; that particular act was not intrusive since NINS, the owner of the desktop computer, provided permission for McIntyre to search. Once McIntyre signed onto the desktop using Christie's password, she performed a search for "Ian Ker's name" in the computer's Mail Application. *See* McIntyre Dep., T37:17-24. McIntyre testified that she did so in order to "locate the date that Father Ker mentioned that he could probably come to NINS, to be our presenter for our fall conference." *Id.* The search results, according to McIntyre's uncontroverted testimony, populated numerous e-mail strands that included the name "Ian Ker." *Id.* at T38:18-20. McIntyre, then, proceeded to read e-mails to find the relevant ones; McIntyre testified that she read under ten e-mails.[15] *Id.* at T38:21-T39:2. McIntyre further testified that she stopped searching after she read an e-mail strand in which Plaintiff apparently spoke "ill of the institute" to Father Ker, and that same e-mail strand also included the date information which McIntyre was searching. *Id.* at T39:8-15, T40:7-25. Importantly, McIntyre testified that when she

[15] Plaintiff's expert opined that 90 minutes after McIntyre was signed onto the desktop, over 40 personal e-mails from Plaintiff's r.christie@att.net account were "accessed" in a matter of two seconds. But, Plaintiff has not provided evidence to show that McIntyre, or someone else at NINS, read those e-mails. It defies logic that someone can review large number of e-mails within a matter of seconds. Rather, the type of "accessing," was a continuation of the automatic downloading process, particularly since McIntyre testified that she did not shutdown the desktop computer when she completed her search of the e-mails. In any event, Plaintiff has not identified specific e-mails, other than the ones involving Father Ker, which Defendants had read.

read the e-mails, she was not aware that some of them were sent and received by Christie through his personal e-mails. *Id.* at T51:20-21.

Plaintiff takes issue with McIntyre's testimony. Essentially, Plaintiff claims that some of McIntyre's statements regarding her lack of awareness that she was reading Christie's personal e-mails, are not credible. First and foremost, other than insinuating that McIntyre provided false testimony, Plaintiff has not proffered any evidence that would tend to contradict McIntyre's statements in this context. To defeat summary judgment, Plaintiff cannot simply assert that testimony is false, without providing some evidence to challenge its veracity. *See Trivedi v. Slawecki*, No. 11-2390, 2014 U.S. Dist. LEXIS 167250, at *37 (M.D. Pa. Dec. 3, 2014)(finding summary judgment appropriate when the plaintiffs failed to provide evidence showing falsity of the statements of a witness); *see also Gonzalez v. Sec'y of Dep't of Homeland Sec.*, 678 F.3d 254, 263 (3d Cir. 2012); *Kirleis v. Dickie, McCamey & Chilcote, P.C.*, 560 F.3d 156, 161 (3d Cir. 2009).

But, more to the point, whether McIntyre was aware that she was reading Christie's personal e-mails is not dispositive. What is more probative is that Plaintiff has failed to show that NINS *intentionally* invaded his privacy. Because invasion of privacy is an intentional tort, an essential element of the claim is that the defendant intentionally invaded a plaintiff's privacy. *See Ehling*, 961 F.Supp. 2d at 674. Indeed, this is not a case where a defendant-employer intentionally accessed an employee's

personal e-mail account, with the knowledge that it may intrude on the personal affairs of another. Rather, the undisputed facts show that personal e-mails read by McIntyre were automatically downloaded onto the NINS desktop — a synchronization process that Christie, himself, permitted and initiated. In other words, McIntyre did not take any action to retrieve those e-mails by unlawful means; the e-mails were passively transmitted onto the desktop.[16]

Although summary judgment as to the claim for invasion of privacy is appropriate because Plaintiff has failed to show an intentional act on the part of Defendants, I also find that Plaintiff did not have any reasonable expectation of privacy as to the personal e-mails that were downloaded onto the NINS desktop computer. First, I start with the principle that the New Jersey Supreme Court has expounded: a plaintiff bears a heavy burden in proving that an invasion of privacy has occurred. *Stengart*, 201

---

[16] Relying on *Stengart*, Plaintiff argues that this Court must consider certain factors in order to evaluate whether an employee has a reasonable expectation of privacy in his/her personal files or e-mails stored on a company computer. *See Stengart*, 201 N.J. at 319. But, *Stengart* and other cases it cites are distinguishable on the basis that they dealt with intentional access of an employee's personal files. For example, in *Stengart*, an employee filed a wrongful termination suit against her former employer. In the course of the litigation, the defendant-employer reviewed personal e-mails between the plaintiff and her attorney that were unintentionally stored on the company computer. The Supreme Court held that pursuant to the strong public policy of protecting attorney-client communications, the plaintiff had a reasonable expectation of privacy in the e-mails that she exchanged with her attorney. *Id.* at 322. This is not the case here; there is no evidence of an intentional act committed by NINS agents to retrieve Plaintiff's personal e-mails, and certainly, the e-mail strand at issue does not implicate any attorney-client privilege.

N.J. at 316-17. Evaluating Plaintiff's claim through that lens, I cannot find that an objective person would reasonably expect privacy in personal e-mails that were downloaded onto a company computer, particularly since Plaintiff made the very decision to do so. Indeed, Plaintiff has not cited to any cases that have found an employer liable for invasion of privacy in this context. Because Plaintiff does not have a reasonable expectation of privacy, correspondingly, I find that Plaintiff has also failed to show that Defendants' conduct was highly offensive.

Accordingly, Defendant's motion for summary judgment is granted as to Plaintiff's invasion of privacy claim.

V. Stored Communications Act

Finally, Plaintiff brings a claim pursuant to the SCA, accusing Defendants of illegally accessing a "facility" in which his electronic communications are stored. *See* Am. Compl., ¶ 43. Essentially, Plaintiff's SCA claim is based on the same wrongful conduct as his invasion of privacy claim: the viewing of Plaintiff's personal e-mails stored solely on the NINS desktop computer. *See* Pl. Reply Brief, p. 13 ("Plaintiff will concede that McIntyre did not access the Yahoo! server to obtain email correspondence between Christie and Father Ian Ker."). Plaintiff's SCA claim does not survive summary judgment for the simple reason that the e-mails Plaintiff alleges that Defendants accessed were stored on a desktop computer, not in a "facility" within the scope of the SCA.

Title II to the Electronic Communications Privacy Act of 1986, also known as the Stored Wire and Electronic Communications and Transactional Records Access, or otherwise known as the Stored Communications Act, 18 U.S.C. §§ 2701-2711, bars unauthorized access to stored electronic communications. Section 2701 includes in relevant part that whoever:

> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility;
>
> and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."

18 U.S.C. § 2701(a). In addition to criminal penalties, the SCA provides a civil cause of action for "any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter." 18 U.S.C. § 2707(a). "Electronic storage" is defined as either "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Congress enacted the SCA, *inter alia*, to protect privacy interests in personal and proprietary information from the mounting threat of computer hackers "deliberately gaining access to, and sometimes tampering with, electronic or wire communications" by means of electronic

trespass. *Thompson v. Ross*, No. 10-479, 2010 U.S. Dist. LEXIS 103507, at *10 (W.D. Pa. Sep. 30, 2010)(citing S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555 at 3557). Pursuant to that purpose, the conduct proscribed by § 2701 is two-fold. First, it is unlawful to access a facility through which electronic communications service is provided, and thereby further obtains, alters, or prevents authorized access of an electronic communication "while it is in electronic storage in such system." 18 U.S.C. § 2701(a). Second, "[i]t is not enough for the electronic communication data to have been accessed in any format on any computer, in order to run afoul of the SCA, the data must have been accessed or obtained while it was within the electronic storage of the electronic communications service itself." *Thompson*, 2010 U.S. Dist. LEXIS 103507, at *10.

Importantly, relevant to this case, the SCA's protection does not extend to e-mails and messages stored only on a personal computer, and not a server. *See In re Google Inc.*, 806 F.3d 125, 146 (3d Cir. 2015)(holding that consistent with the plain meaning of the SCA, "an individual's personal computing device is not a facility through which an electronic communications service is provided")(citations and quotations omitted); *Allen v. Quicken Loans, Inc.*, No. 17-12352, 2018 U.S. Dist. LEXIS 192066, at *31 (D.N.J. Nov. 9, 2018)("[b]ecause under the SCA an individual's personal computer or device is not a facility through which an electronic communications service is provided, [plaintiff's] SCA claim

fails"); *Thompson*, 2010 U.S. Dist. LEXIS 103507, at *15-16 ("e-mail messages downloaded and stored on, and subsequently accessed solely from, a user's personal computer does not fit within the SCA's definition of electronic storage"); *Bailey v. Bailey*, No. 07-11672, 2008 U.S. Dist. LEXIS 8565, at *17 (E.D. Mich. Feb. 6, 2008); *In re Doubleclick Inc.*, 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001)("the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not 'electronic communication service' providers"); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017)(finding that personal computers are not covered by the SCA); *Gracia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012)(finding that a computer of an end user is not protected by the SCA); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1104 (9th Cir. 2014).

Here, the e-mails which Plaintiff claims were illegally accessed by Defendants were retrieved from storage within the hard drive of the NINS desktop, not from the electronic communication service provider's own storage. Based on the record, Plaintiff has not shown that Defendants accessed e-mail communications directly from any kind of storage operated and maintained by internet service providers, or more specifically, Yahoo! or att.net, with which Plaintiff had e-mail accounts and received e-mail services. Absent a showing that Defendants accessed Plaintiff's personal e-mails through such a service provider or equivalent, Plaintiff's claim under the SCA cannot stand.

None of Plaintiff's cited authorities stand for a contrary conclusion. For example, Plaintiff cites to *Hoofnagle v. Smyth-Wythe Airport Comm'n*, No. 15-08, 2016 U.S. Dist. LEXIS 67723 (W.D. Va. May 24, 2016), for the proposition that the unauthorized access of an employee's personal e-mail account violates the SCA. *Id.* at *26-28. However, that case is inapposite because it involved a former employer that accessed e-mails stored on the employee's Yahoo! account — not copies of e-mails stored in an individual work computer owned by the employer. The case law is clear: a computer of an end user is not protected by the SCA, regardless whether the e-mails were downloaded from a remote server. *See In re Google Inc.*, 806 F.3d at 146 ("The origin of the Stored Communications Act confirms that Congress crafted the statute to specifically protect information held by centralized communication providers."); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003)("the [SAC] clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system," but that the Act "does not appear to apply to the [government's] source's hacking into [the plaintiff's personal] computer . . . because there is no evidence that [the] computer maintained any 'electronic communication service[.]'").

Similarly, Plaintiff's reliance on *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2003), is inapt, because that case also concerned a former employer obtaining access to e-mails stored on the servers of an e-mail service provider. *Id.* at 1071. Additionally, Plaintiff mistakenly relies on

Ehling, as that case dealt with the issue whether accessing a Facebook post stored on Facebook servers is prohibited by the SCA. *Ehling*, 961 F. Supp. 2d at 666. While the *Ehling* Court found the Facebook server is within the scope of the SCA, that case decidedly did not involve e-mails stored on a desktop computer. Accordingly, Plaintiff's SCA claim is dismissed, and Defendants' motion for summary judgment is granted as to this cause of action.

Having analyzed all of Plaintiff's claims, I find that summary judgement is appropriate as to all the claims. Thus, Defendants' motion is granted in its entirety; Plaintiff cross-motion for summary judgment as to his claims is denied.

VI. NINS's Counterclaims

Defendants assert three counterclaims against Plaintiff related to Plaintiff's alleged wrongful retention of Defendants' laptop computer: (1) replevin; (2) bailment; and (3) unjust enrichment. Without individually discussing each claim, Plaintiff argues, on mootness grounds, that summary judgment is appropriate on all the counterclaims, because he has already returned the laptop, and that the sole reason why he kept the laptop is because of this litigation. I will address each claim below.

A. Replevin

Under New Jersey law, replevin is governed by N.J.S.A. 2B:50-1, *et seq.* Pursuant to N.J.S.A. 2B:50-1, "[a] person seeking recovery of goods wrongly held by another may bring an action for replevin . . . . If the person

establishes the cause of action, the court shall enter an order granting possession." *Id*; *Auto. Fin. Corp. v. DZ Motors*, LLC, No. 16-7955, 2017 U.S. Dist. LEXIS 120154, at *6-7 (D.N.J. Jul. 26, 2017). To succeed in a replevin action, the burden is on plaintiff to establish absolute ownership and right to the possession of the property. *Mandelbaum v. Weiss*, 11 N.J. Super. 27, 30-31 (App. Div. 1950); *see also Hunt v. Chambers*, 21 N.J.L. 620, 623 (E. & A. 1845)("To maintain replevin, the plaintiff must have the right of exclusive possession to the goods in question. He must not only have property absolute or qualified, and the right of possession at the time of the commencement of the action, but he must have the exclusive right of possession."); *Mehrnia v. Emporio Motor Group, LLC*, No. Ber-C-264-14, 2016 N.J. Super. Unpub. LEXIS 415 (App. Div. Feb. 25, 2016). Importantly, and relevant here, "[w]hen one has wrongfully detained property and refused it on demand he is liable in an action in replevin even though it may not remain in his possession when the suit is brought." *Baron v. Peoples Nat'l Bank*, 9 N.J. 249, 257 (1952).

Here, it is undisputed that NINS owned the laptop computer, and that Plaintiff was given permission to use the laptop for work purposes. When Plaintiff left NINS, Defendants repeatedly sought the return of the laptop from Plaintiff. While the laptop was ultimately returned to NINS by Plaintiff during the course of this litigation, the fact that the laptop was returned does not moot Defendants' replevin counterclaim. *See Baron*, 9 N.J.at 257. In such a situation, the claim of replevin would not be an

action for the return of specific chattels, but for their value and damages for the unlawful detention. *Id.* As such, Plaintiff's summary judgment as to Defendants' replevin counterclaim is denied.

B. Bailment

Although Defendants do not explicitly allege conversion, in New Jersey, a bailor may sue a bailee in conversion and/or negligence. Common law conversion is "the exercise of any act of dominion in denial of another's title to the chattels or inconsistent with such title." *Mueller v. Technical Devices Corp.*, 8 N.J. 201, 207 (1951). Thus, intentional or negligent acts can give rise to a conversion cause of action. *Lembaga Enterprise, Inc. v. Cace Trucking & Warehouse, Inc.*, 320 N.J. Super. 501, 507 (App. Div. 1999). "The tort arises from the bailee's commission of an unauthorized act of dominion over the bailor's property inconsistent with its rights in that property." *Id.* The good faith or intent of the bailee do not play a part in an action for conversion. *McGlynn v. Schultz*, 90 N.J.Super. 505, 526 (Ch. Div. 1966), *aff'd,* 95 N.J. Super. 412 (App. Div.), *certif. denied*, 50 N.J. 409 (1967). For example, a bailee who mistakenly destroys or disposes of the goods is liable in conversion although there is no intent to steal or destroy the goods. Indeed, conversion can be brought to seek damages arising from the exclusion of an owner's rights. *See Barco Auto Leasing Corp. v. Holt*, 228 N.J. Super 77, 83 (App. Div. 1988); *McGlynn*, 90 N.J. Super at 526; *Winkler v. Hartford Accident and Indemnity Co.*, 66 N.J. Super. 22 (App. Div.1961), *certif. den*ied, 34 N.J. 581 (1961); *Taylor v.*

Brewer, 94 N.J.L. 392, 393 (N.J. 1920); *Winkler v. Harford Acci. & Indem. Co.*, 66 N.J. Super. 22, 29 (App. Div. 1961)("After an act of conversion has taken place and become complete, even an unconditional offer to return the goods or actual return of the goods does not bar the cause of action, although it may tend to mitigate damages.").

Based on the well-established law of New Jersey in this context, a conversion claim based on a bailor-bailee relationship does not extinguish simply because the property was returned to the rightful owner. As such, contrary to Plaintiff's argument, Defendants' bailment/conversion claim is not mooted by the return of the laptop. This counterclaim, too, survives Plaintiff's summary judgment motion.

C. Unjust Enrichment

To state a claim for unjust enrichment, a party must allege (1) at plaintiff's expense (2) defendant received benefit (3) under circumstances that would make it unjust for defendant to retain benefit without paying for it. *In re K-Dur Antitrust Litigation*, 338 F.Supp. 2d 517, 544 (D.N.J. 2004) (citing Restatement of Restitution § 1 (1937)). Restitution for unjust enrichment is an equitable remedy, available only when there is no adequate remedy at law. *National Amusements, Inc. v. N.J. Tpk. Auth.*, 261 N.J. Super. 468, 478 (Law Div.1992), *aff'd*, 275 N.J. Super. 134 (App. Div. 1994). To establish a claim for unjust enrichment under New Jersey law, a plaintiff must prove both that defendant received a benefit and that retention of that benefit without payment would be unjust." *VRG Corp. v.*

GKN Realty Corp., 135 N.J. 539, 554 (1994). In addition, the unjust enrichment doctrine requires that a plaintiff show that it "expected remuneration from defendant at the time it performed or conferred a benefit on defendant" and that the "failure of remuneration enriched defendant beyond its contractual rights." *Id.*

Here, the Court finds that the unjust enrichment claim fails as a matter of law. There is simply no evidence that Defendant expected Plaintiff to compensate NINS for the usage of the company laptop. Indeed, Plaintiff was provided the laptop in the normal course of employment to facilitate his work at NINS. In that connection, Defendants did not confer any benefits upon Plaintiff, since there is no evidence that Plaintiff used the laptop for any purpose other than his employment with NINS. I find summary judgment appropriate on this counterclaim.

In conclusion, I stress that my decision to deny Plaintiff's summary judgment as to Defendants' replevin and bailment counterclaims is solely made in the context of mootness — the only argument Plaintiff has made in favor of granting his motion. I, therefore, express no opinions as to whether Defendants have sufficiently proven their remaining counterclaims on the merits, particularly since the parties have not adequately briefed the issues. At this time, only those surviving counterclaims can proceed.

CONCLUSION

For the reasons set forth above, Defendants' motion for summary judgment is **GRANTED**. Plaintiff's cross-motion for summary judgment as to his claims is **DENIED**. Plaintiff's motion for summary judgment as to Defendants' counterclaims is **GRANTED** in part and **DENIED** in part, as follows: Defendants' replevin and bailment counterclaims survive summary judgment; however, their unjust enrichment counterclaim is dismissed.

An appropriate order shall issue.

DATED: April 30, 2019

/s/ Freda L. Wolfson
Freda L. Wolfson
U.S. District Judge